REMARKS/ARGUMENTS

Favorable reconsideration of this application for the reasons noted hereinafter is respectfully requested.

Claims 1-18 are pending in this application, Claim 1 having been presently amended. Support for amended Claim 1 can be found, for example, in the original claims, drawings, and specification.[1] No new matter has been added.

In the outstanding Office Action, Claims 1-18 were rejected under 35 U.S.C. § 102(b) as anticipated by Akachi (U.S. Patent No. 7,069,436, hereinafter "Akachi").

In response to the rejection of Claims 1-18 under 35 U.S.C. § 102(b) as anticipated by Akachi, Applicant has amended Claim 1 to recite novel features clearly not taught or suggested by the applied references.

Amended independent Claim 1 is directed to a wireless ad-hoc communication system including, *inter alia*:

> . . . a first terminal configured to encrypt a payload of a broadcast frame and to transmit the broadcast frame; and
>
> a second terminal configured to receive the broadcast frame and to decode the payload of the broadcast frame, wherein
>
> the first terminal is configured to encrypt the payload of the broadcast frame using a broadcast encryption key assigned to the first terminal,
>
> the second terminal is configured to decode the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal, and
>
> any terminal in the plurality of terminals may perform the role of said first terminal or said second terminal.

[1] See page 16, line 25 to page 17, line 12 and page 28 lines 12-19 of the specification; and in Figures 1 and 9.

By way of background, Applicant's Claim 1 is directed to a wireless ad-hoc communication system in which the terminals are always moving. The terminals frequently participate in or are disconnected from a network, and therefore, terminals constituting a broadcast group cannot be fixed. Thus, an advantageous feature of a non-limiting embodiment of the Applicant's invention is that participants may join or leave the wireless communication system on an ad-hoc basis.

Turning now to Akachi, Akachi describes "an information transmission system and method, transmitting apparatus, and receiving apparatus for delivering information over a transmission path, such as via a satellite."[2] Thus, Akachi describes one-way satellite communication in which the subscribers (the receivers) receive data from the transmitter, through the satellite but cannot transmit data to the satellite. In contrast, in Applicant's Claim 1, the subscribers have the ability to intercommunicate.

In Claim 1, the first terminal (i.e. sending terminal) encrypts the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal, and the second terminal decodes the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal. In essence, this provides independent and distributed management of broadcast encryption keys, wherein the key neither need be common to several terminals nor be managed at one location.

In Akachi, the reception terminal decodes the packets using a ***common key which is common to a plurality of reception terminals*** as the decoding key for a broadcast,[3] rather

[2] See Akachi at column 1, lines 10-13.
[3] See Akachi at column 8, lines 36-38.

than the broadcast encryption key assigned to the sending terminal, as in Applicant's Claim 1 because, in satellite communication, there is only one transmitter for the subscribers. However, in an ad-hoc communication network, there are several transmitters for a subscriber, and each respective transmitter has a broadcast encrypt key.[4]

Accordingly, Applicant respectfully submits that independent Claim 1 (and all claims depending thereon) patentably distinguishes over Akachi.

Independent Claim 4 recites, *inter alia*:

> . . . an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key assigned to the different terminal;
>
> means for searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a received broadcast frame to extract the corresponding broadcast encryption key; and
>
> means for decoding a payload of the broadcast frame using the extracted broadcast encryption key.

Independent Claims 5 and 11 recite substantially similar features as independent Claim 4. Thus, the arguments presented below with respect to independent Claim 4 are applicable to independent Claims 5 and 11.

Akachi fails to teach or suggest "an encryption-key management list table having at least one encryption-key management list comprising a set of a terminal identifier of a different terminal and a broadcast encryption key assigned to the different terminal." Rather, Claim 11 of Akachi describes that:

---

[4] For example, a non-limiting embodiment of Applicant's invention shown in Figure 13, shows items 226, BK_B, BK_C, and BK_D.

> . . . wherein a table is searched to determine whether said ***read address*** indicates that said portion of said received data is intended for ***said group*** [***the receivers***] or is intended solely for said respective one of said plurality of ***processing devices*** [***the receiver***], and when said portion of said received data is encrypted, said table is again searched to locate said stored address that coincides with said read address and then a decryption key corresponding to said stored address is retrieved, said decryption key being retrieved only when a stored value associated with said decryption key indicates that said decryption key is in a valid state.

Thus, Akachi describes that the read address belongs to the receiver rather than the transmitter. Whereas, in Applicant's Claim 4, the "terminal identifier of a different terminal and a broadcast encryption key assigned to the different terminal" belong to the transmitter, not to the receivers.

Additionally, Akachi fails to teach or suggest a "means for searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a ***received broadcast frame*** to extract the corresponding broadcast encryption key," as recited in Claim 4. Column 13, lines 36-44 of Akachi states that "when it is necessary to encrypt the data located in the payload, such as for an IP packet, the ***transmission processing device*** *113* retrieves an encryption key assigned to the MAC address of the terminal 124i for arrangement within the section header. The encryption key is retrieved from the encryption key table stored in the encryption key table storage unit 113A and is used to encrypt an IP packet arranged in the payload of that section." Thus, the process in Akachi is done in the ***transmitter terminal,*** and is not done in the ***receiver terminal.***

Furthermore, Claim 5 recites a terminal comprising "an encryption-key management list table having at least one encryption-key management list configured to ***store a unicast encryption*** key between said terminal and a different terminal ***and a broadcast encryption key*** assigned to the different terminal in association with a terminal identifier of the different terminal," and is further believed to be patentable for the reasons discussed next.

Applicant respectfully submits that an additional advantageous feature of non-limiting embodiment of Applicant's invention is the use of two kinds of encryption keys for one receiver/transmitter. Applicant's invention stores "a unicast encryption key between said terminal and a different terminal and a broadcast encryption key assigned to the different terminal," as recited in Claim 5. However, Claim 11 of Akachi merely recites "whether said ***read address*** indicates that said portion of said received data is intended for ***said group*** [***the receivers***] or is intended solely for said respective one of said plurality of ***processing devices*** [***the receiver***]." Thus, Akachi does not describe that the transmitter/receiver will adopt a different encryption key when the transmission is directed to a group of users or a sole user.

Claim 2 recites a "means for decoding the payload of the broadcast frame ***using the extracted broadcast encryption key assigned to the first terminal***," and is also believed to be patentable for at least the reasons discussed above with regard to Claims 4, 5, and 11. Claim 2 is further believed to be patentable for the reasons discussed next.

Column 6, lines 47-52 of Akachi states that "the decoding unit 34 refers to a key table 37, ***using the MAC address of the information processing device 22***, to obtain a decoding key from the key table 28. The decoding unit 34 then decodes the data stream D31 using the decoding key and supplies the resultant decoded data D34 to the checker 35." The decoding

key in Akachi is obtained according to the MAC address of the reception system. Thus, ***the encryption key is not assigned to the first terminal*** (i.e. transmission terminal), as in Claim 2.

Accordingly, Applicant respectfully submits that Claims 2, 4, 5, and 11 patentably distinguish over Akachi.

Claim 3 recites a terminal including, *inter alia*, "a generated-key table configured to store the broadcast encryption key assigned to the first terminal." Independent Claims 6 and 7 recite substantially similar features as Claim 3. Thus, the arguments presented below with respect to Claim 3 are applicable to independent Claims 6 and 7.

Akachi describes that the encryption key table maintained in the transmission processing device 113 is for storing an encryption key table in the form of a diagram oriented to the encryption key assigned to ***each MAC address***.[5] In contrast, in Claim 3, the generated-key table of the terminal stores the encryption key of ***the terminal itself***. Thus, Akachi fails to teach or suggest "a generated-key table configured to store the broadcast encryption key assigned to the first terminal," as in Claim 3.

Accordingly, Applicant respectfully submits that Claims 3, 6, and 7 patentably distinguish over Akachi.

Independent Claim 8 recites a "means for encrypting a terminal identifier and a broadcast encryption key of the terminal using a unicast encryption key assigned to a transmission-destination terminal." Independent Claim 9 recites substantially similar features

[5] See Akachi at column 13 lines 16-19.

as independent Claim 8. Thus, the arguments presented below with respect to independent Claim 8 are applicable to independent Claim 9.

Column 1, lines 24-29 of Akachi describes a ***common key***, but does not describe a ***unicast encryption key***. Thus, Akachi fails to teach or suggest the encryption of a broadcast encryption key using a unicast encryption key.

Accordingly, Applicant respectfully submits that the independent Claims 8 and 9 patentably distinguish over Akachi.

Independent Claim 12 recites a method for "encrypting a broadcast frame in a terminal that includes a generated-key table storing a broadcast encryption key assigned to said terminal." Independent Claim 16 recites substantially similar features as independent Claim 12. Thus, the arguments presented below with respect to independent Claim 12 are applicable to independent Claim 16.

As discussed above with regard to Claims 3, 6, and 7, Akachi fails to teach or suggest encrypting a broadcast frame in a terminal that includes "a generated-key table storing a broadcast encryption key of said terminal."

Accordingly, Applicant respectfully submits that the independent Claims 12 and 16 also patentably distinguish over Akachi.

Independent Claim 13 recites a "receiving a terminal identifier and a broadcast encryption key that are encrypted ***using a unicast encryption key between the first terminal and the second terminal***" and "decoding . . . ***using the unicast encryption key***;" and "encrypting a terminal identifier . . . ***using the unicast encryption key***." Independent Claims 14, 17, and 18 recite substantially similar features as independent Claim 13. Thus, the

arguments presented below with respect to independent Claim 13 are applicable to independent Claims 14, 17, and 18.

In contrast, column 1, lines 24-29 of Akachi describes encryption by a common key and fails to teach or suggest the use of a unicast encryption key to encode the common key.

Accordingly, Applicant respectfully submits that the independent Claims 13, 14, 17, and 18 patentably distinguish over Akachi.

Independent Claim 10 recites a "means for encrypting the terminal identifier and the broadcast encryption key of the different terminal using a broadcast encryption key assigned to the terminal," and is thus believed to be patentable for at least the reasons discussed above with regard to independent Claims 14 and 18. Claim 15 recites substantially similar features as Claim 10 and is also believed to be patentable.

Claim 10 is further believed to be patentable for at least the reasons discussed next. Column 1, lines 24-29 of Akachi describes encryption using a common key and fails to teach or suggest using the broadcast key of a receiving terminal to encrypt or encode the broadcast key of the transmitting terminal.

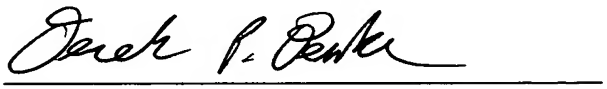
Accordingly, Applicant respectfully submits that the independent Claims 10, 14, and 18 patentably distinguish over Akachi.

Thus, Applicants respectfully request that the rejection under 35 U.S.C. § 102(b) as anticipated by Akachi be withdrawn.

Consequently, in view of the above comments, it is respectfully submitted that the outstanding grounds for rejection have been overcome and that Claims 1-18 patentably distinguish over Akachi. Claims 1-18 are therefore believed to be in condition for allowance, and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Derek P. Benke
Registration No. 56,944

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)